AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Nebraska

SEALED

United States of America
v.

JUDE UZOCHUKWU IFEANYI

Defendant(s)

Case No. 8:18MJ433

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 23, 2018 in the county of Douglas in the _____ District of Nebraska, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S. Code § 1343	fraud by wire, radio, or television
18 U.S.C. § 1030(a)(4)	accessing protected computer in furtherance of fraud
18 U.S.C. § 2	Aiding and Abetting

This criminal complaint is based on these facts:

See affidavit

☑ Continued on the attached sheet.

Complainant's signature

FBI SA Jacob Foiles

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/19/2018

Judge's signature

City and state: Omaha, Nebraska

Michael D. Nelson, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA v. JUDE UZOCHUKWU IFEANYI	**Filed Under Seal**

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Jacob Foiles, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a criminal complaint against Jude Uzochukwu Ifeanyi (IFEANYI).

2. I am presently employed as a Special Agent of the Federal Bureau of Investigation (FBI), and am assigned to the Cyber Task Force of the Omaha Field Office in the District of Nebraska. I have been employed by the FBI since October 2014, including five months of training at the FBI Academy in Quantico, Virginia. Subsequent to my initial training at the FBI academy I have received additional training in the investigation of computer and financial crimes. Previous to my employment with the FBI, I obtained a Bachelors degree in Computer Engineering, and was employed in the information technology industry for seven years. As a result of my training and experience, I am familiar with information technology and its use in criminal activities.

3. The facts in this affidavit come from information obtained from my investigation, from my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (fraud by wire, radio, or television), 18 U.S.C. § 1030(a)(4) (accessing protected computer in furtherance of fraud) and 18 U.S.C. § 2 (Aiding and Abetting) have been committed by IFEANYI.

PROBABLE CAUSE

1. I am investigating a successful Business Email Compromise (BEC)[1] that resulted in the transfer of $700,000 to a fraudulent bank account. The victim of the BEC, identified by the initials D.P., LLC, is a business in Omaha, Nebraska that is owned by T.D. and J.D[2].

2. In May 2018, T.D and J.D. exchanged several emails with another couple, K.T. and T.T., about purchasing K.T. and T.T.'s ownership of a jointly owned condominium in Florida. T.D and J.D. agreed to send $700,000 via wire transfer to K.T. and T.T. in order to purchase K.T. and T.T.'s share of the condominium. T.D. and J.D. each have an email account associated with their business, D.P., LLC hosted on Microsoft's Office365[3] platform. K.T. and T.T. each have an email account hosted on Google's free Gmail platform.

3. On May 23, 2018 at approximately 10:11 AM K.T. sent an email to both T.D and J.D. containing their Bank of America account information. At approximately 11:31 AM, T.D and J.D. received another email that appeared to be from K.T.'s legitimate email address that asked if they could

---

[1] Business Email Compromise (BEC) is a sophisticated scam targeting businesses and individuals that regularly perform wire transfer or ACH payments. A BEC scammer attempts to use email in order to defraud a business or individual of money.

[2] The names and personal details of the individuals involved in this investigation have been replaced by their initials to protect their identities.

[3] Office 365 is a cloud-based hosted email platform developed by Microsoft. Office 365 allows organizations to use a custom domain name, rather than a Microsoft owned domain like *outlook.com*.

instead use a different bank account. This email was later determined to be fraudulent – it was not sent by K.T.

4. At approximately 12:24 PM, T.D and J.D. received another email that appeared to be from K.T.'s legitimate email address that provided the following "alternate wiring instructions":

Direct the wire to: Chase Bank
2048 Bakersmill Rd. Davula, GA 30019
Routing No: 322271627

For final credit to: THC CO
Account No: xxxxxx536

5. On May 23, 2018, T.D and J.D. went to Northwest Bank in Omaha, Nebraska and requested a $700,000 wire transfer be submitted to Chase Bank account # xxxxxx536.

6. On May 25, 2018, T.D. received a call from a fraud investigator at JP Morgan Chase who asked T.D. to verify if the intended recipient (K.T. and T.T. in this case) had received the funds. T.D and J.D. then contacted K.T. and T.T. and realized that they had submitted the wire transfer to a fraudulent bank account and proceeded to contact their bank and law enforcement.

7. Records provided by Chase Bank pursuant a subpoena indicate that the recipient of the $700,000 wire transfer, S.T., is a 19 year old who resides in Los Angeles, California. These records indicate that on May 23rd and May 24th 2018, S.T. withdrew approximately $383,000 from several different Chase Bank locations as both cash and cashier's checks. Ultimately, Chase Bank was able to return $568,515 of the $700,000 to T.D and J.D.

8. K.T. and T.T. provided the FBI with copies of the emails sent and received by both parties during the time of this incident. As is described in detail below, the FBI's analysis of these emails

and their headers[4] indicates that J.D.'s Microsoft Office 365 email account was compromised and accessed by someone who learned of the condominium buyout and impersonated both K.T. and J.D.

9. Four (4) fraudulent emails were sent to T.D and J.D. between May 23 and May 25, 2018, all of which were spoofed so that they appeared to come from K.T.'s legitimate Gmail address. A spoofed email is a message that is crafted with a forged sender address. These emails had a "From" address that matched K.T.'s legitimate email address, but used a "Reply-To" address[5] that took K.T.'s legitimate email address and added "*@emailreplysecurity.com*" to the end. Additionally, the emails contained a "CC" address that took T.T.'s legitimate email address and added "*@emailreplysecurity.com*" to the end. This caused J.D. and T.D.'s replies to be sent to fraudulent email addresses with the domain[6] *emailreplysecurity.com* rather than to K.T. and T.T.'s email addresses. The domain *emailreplysecurity.com* is registered at Namecheap, Inc.[7] Emails sent to addresses within the *emailreplysecurity.com* domain are directed to Namecheap's email servers.

10. Queries of FBI databases have revealed at least ten (10) other companies or individuals targeted by similar BEC schemes that also reported receiving emails that contained the domain '*emailreplysecurity.com*'. Based on these other reports and my training and experience, it appears that the subject(s) responsible for defrauding T.D and J.D. have likely targeted other victims and appear to use

---

[4] An email header contains control and diagnostic information that shows where an email originated from, how it arrived at its destination, and other details. An email header is used by email systems to correctly deliver and track messages.

[5] The "Reply-To" address is the email address that will be used if the recipient replies to the sender. Most emails have the same "From" and "Reply-To" addresses.

[6] A domain name is an identification string that defines a realm of administrative autonomy, authority or control within the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS). Examples of domains include "fbi.gov", "google.com", and "yahoo.com". Domain names are registered and managed by domain name registrars.

[7] Namecheap is a web hosting company in Phoenix, Arizona that provides domain registration, website and email hosting, and other internet services

email addresses with the domain '*emailreplysecurity.com*' to communicate with those victims.

11. Additionally, the fraudulent emails sent to T.D and J.D. also contained an "X-Originating-IP" of 45.35.132.200. The "X-Originating-IP" attribute is used by email systems to record the IP address[8] of the user that originally sent the email. This IP address is assigned to SmartHost, LLC, a web hosting company based in Henderson, Nevada. The FBI contacted SmartHost and determined that IP address 45.35.132.200 was assigned by SmartHost to a customer named "Web Pundits" based in India.

12. Web Pundits sells Remote Desktop ("RDP") and web hosting services. A RDP service provides a user with the ability to connect to a remote computer and use it like their local computer. In my training and experience, RDP services are frequently used by cyber criminals to obfuscate their illegal activity and gain access to websites or other online resources that might block access from the cyber criminal's country. The FBI contacted Web Pundits and provided the exact dates and times of the four (4) fraudulent emails that were sent to T.D and J.D. that contained the IP address of 45.35.132.200. Using this information, Web Pundits was able to identify a single user that had activity during all of those dates and times. Web Pundits provided the following details for this user:

> Name: Lord Iphie
> Email: uzohifeanyi@outlook.com
> Phone: +234.7066920566
> IP used while making order onto our website: 154.73.11.9
> Account created on February 4

13. Three (3) fraudulent emails were sent to K.T. and T.T. between May 23 and May 25, 2018, all of which appear to have been sent from J.D.'s legitimate Office 365 account. These emails all contained a "CC" address that took T.D.'s legitimate email address and added "*@emailreplysecurity.com*" to the end.

---

[8] An Internet Protocol (IP) address is a unique number assigned to devices that enables them to connect to networks and the internet.

14. The fraudulent emails sent to K.T. and T.T. contained an "X-Originating-IP" of 154.73.11.9. This is the same IP address used by "Lord Iphie" when placing an order at Web Pundits listed in the paragraph above. The fact that the IP address found in the fraudulent emails sent to K.T. and T.T. matches the IP address provided by Web Pundits indicates that the email address *uzohifeanyi@outlook.com* and phone number +234.7066920566 provided by Web Pundits are connected to the subject(s) that defrauded T.D and J.D. This IP address, 154.73.11.9, is assigned to Tizeti, an internet service provider (ISP) in Nigeria. The country code +234 is used to place calls to Nigeria.

15. On June 6, 2018, S.P. from C.S. Inc., the company that provides IT support for D.P. LLC, J.D. and T.D.'s company, discovered configuration changes made to J.D.'s Office 365 email account that were not made by J.D. or C.S. Inc. One of these changes enabled email forwarding to the email address *judejude754@gmail.com*. Essentially this would have caused every email sent to J.D. to also be sent to *judejude754@gmail.com*. In my training and experience, I know that email forwarding is often configured by BEC scammers in order to direct emails to an account under their control. Often, these rules go undiscovered and can remain in place even after a victim has changed their account password and/or detected the fraudulent activity.

16. In addition to the email forwarding change, email rules were also configured within J.D.'s account. Rules can be created within Office 365 and other email platforms that take automatic actions based on configured triggers. For example, a rule can be configured to move certain messages from a particular email address to a specific folder. In this case, rules were configured that deleted messages from T.T. or K.T.'s legitimate email addresses or contained the email address *judejude754@gmail.com*. These rules were likely created to ensure J.D. did not see any legitimate emails sent from T.T. or K.T or any messages that mentioned the *judejude754@gmail.com* email address.

17. Records and logs were obtained from Namecheap, Inc., pursuant a subpoena, for the *emailreplysecurity.com* domain. This domain was registered by a user that provided the following

information:

> Username: bamiadmin
> Name: bamidele ayo
> Email: hronlinedpt@gmail.com
> Phone: +232.8188513660
> Address: 35 costain ave. lagos

Email logs were also provided by Namecheap which show that emails sent to any address within the *emailreplysecurity.com* domain, to include those referenced above, were forwarded to the email address *abutrading1@gmail.com*. These emails were not stored on any Namecheap systems but were instead automatically forwarded on to this Gmail address.

18. A search warrant was obtained for the Microsoft account *uzohifeanyi@outlook.com* used to register for RDP service with Web Pundits. Analysis of the contents of this account revealed an email that appeared to be a letter written requesting a visa to visit South Africa. The email contained a full name, passport number, address, phone number, and other details. This email was sent from *ifeanyiuzochukwu@icloud.com* to *uzohifeanyi@outlook.com* on June 10, 2018 with the following content:

> CPL
> PROPERTY LT D.
> 8th May, 2018
> The Consular
> South African High Commission,
> 24 Molade Okova Thomas
> Victoria Island,
> Lagos
> Dear Sir/Ma
> SELF INTRODUCTION LETTER
> I am Mr JUDE UZoCHUKwU IFEANYI, a Nigerian and holder of Passport No: A08444445. I am the CEO of the above named company
> 1 hereby apply for an entry clearance visa to make a short visit to your country
> I will be visiting Johannesburg in South Africa from 19h May 2018 to 31st May 2018, and all trip expenses will be made by me.
> Attached are my application evidence of funds and other documentations for your scrutiny sir.
> Thanks.
> Yours faithfully

JUDE U. IFEANYI.
O|
5A James Anyaeche Street
Off UBA Road, Bakare Estate Lekki.
www.ujiandcopropertyltd-ng.com
info@ujiandcopropertyltd-ng.com
sales@ujiandcopropertyltd-ng.com
REAL ESTATE DEVELOPMENT I ARCHITECTURAL DESIGNS 1 FACILITY MANAGEMENT IGENERAL SURVEYS
+234 (0) 9094642540, 803 887 9545

19. A search of FBI databases for the name "Jude Uzochukwu Ifeanyi" and passport # A08444445, revealed that a Nigerian man with the same name, passport, address, phone number, and other details applied for a U.S. visa on August 8, 2018. The details provided by IFEANYI on his visa application included the following:

Name: Jude Uzochukwu Ifeanyi
Passport Number: A08444445
Address: 5A James Anyaeche Street Chevron, Lekki, Lagos, Nigeria
Phone Number: 09094642540
Email Address: ifeanyiuzochukwu@icloud.com
Employer: UJI & CO Property LTD
Spouse: Vivian Oluchi Agbune

20. The FBI identified an email sent from *uzohifeanyi@outlook.com* to *customer.support@jumia.com* on June 30, 2018 with the following message:

An LG Home theatre HT358SD. I bought on 6th of June and was delivered on 10th of June. Stop working on 19th of June, I contacted ur company and a provision was made for a return to LG service centre FUOANI @ Lekki. When I got there yesterday they rejected the product that the LG product I got from your company was a fake LG product.
This is the Order No. 332865296

Included with the email was an image of a sales invoice from Jumia, an online marketplace headquartered in Nigeria, with the following customer details:

Ifeanyi Uzoh
5A James Anyaeche Street, Chevron Estate
CHEVRON
Lagos
Nigeria

This address matches what IFEANYI listed on his U.S. visa application.

21. Subscriber records were requested from Tizeti regarding the IP address 154.73.11.9. Records provided by Tizeti indicate that along with several dozen other customers, the following subscriber used IP address 154.73.11.9 on May 23, 24, and 25, 2018 - the dates that fraudulent emails were sent to K.T. and T.T.:

> Name: Ikenna Okeke
> Address: 4A, James Anyachae str, Chevron estate
> Email: water4all25@icloud.com
> Phone: 2348038879545

This address is nearly identical to the address listed on IFEANYI's U.S. visa application and the Jumia sales invoice for "Ifeanyi Uzoh" described above.

22. WhatsApp[9] accounts were discovered for both the Nigerian phone number listed on IFEANYI's U.S. visa application, +2349094642540, and the number associated with the Tizeti internet subscriber "Ikenna Okeke" listed above, +2348038879545. Both WhatsApp accounts have the following user description dated September 7, 2017:

> *NO MATTER THE ECONOMY OF THE JUNGLE, I CAN NEVER EAT GRASS" ITS NOT PRIDE ITS JUST WHO I AM!!!!!! Lion king*[10]

This description matches the user description found on a Facebook account for the user "Ifeanyi Walter Uzochukwu (The Lion King)". This Facebook account contains a large logo with the text "UJI&CO PROPERTY LTD.", the name of the employer that IFEANYI listed on his U.S. visa application. The WhatsApp account associated with +2349094642540 also contains the same logo with the text

---

[9] WhatsApp is a communication platform owned by Facebook that allows users to communicate with each other via text message or phone call

[10] The descriptions included several emoticons, or small images, of a lion and a crown which were omitted from this affidavit.

"UJI&CO". Several photos uploaded to the Facebook account match the photo associated with IFEANYI's U.S. visa application.

23. An email was found in the *uzohifeanyi@outlook.com* account sent to *internet@wifi.com.ng*, an email address used to contact Tizeti, on June 29, 2018. The email contained the following:

> Userid: Ikenna Okeke
> Email: ifeanyiuzochukwu@icloud.com
>
> I subscribed for network on 24th of June 2018, but the network had issues that was resolved yesterday by ur IT team.
> Am appealing that the subscribed network should start on 28th.
> Thanks

This is further confirmation that the individual(s) using the *uzohifeanyi@outlook.com* account are also using Tizeti's internet service.

24. A search warrant was obtained for the Google account configured to receive copies of all emails sent to J.D.'s email account - *judejude754@gmail.com*. The subscriber information provided by Google for this account is as follows:

> Name: jude jude
> e-Mail: judejude754@gmail.com
> Recovery e-Mail: water4all25@yahoo.com
> SMS: +2349094642540 [NG]

In addition to the account name "jude jude" matching IFEANYI's first name, the SMS number associated with this account is also connected to IFEANYI, as it is the number listed on his U.S. visa application noted in paragraph 19 above. Account login records provided by Google indicate that the email account *judejude754@gmail.com* was accessed from both the IP address found in the fraudulent emails sent to J.D. and T.D. (45.35.132.200) as noted in paragraph 11 above, and the IP address found in the fraudulent emails sent to K.T. and T.T. (154.73.11.9) as noted in paragraph 14 above.

25. Google also provided a list of other accounts linked to *judejude754@gmail.com*. The

email account *vivian.agbune80@gmail.com* was linked to *judejude754@gmail.com* by cookie[11]. *Vivian.agbune80@gmail.com* is the email address that was listed on the U.S. visa application of Vivian Agbune, IFEANYI's wife. Both IFEANYI and his wife Agbune applied for a U.S. visa on August 8, 2018. The email account *abutrading1@gmail.com* that Namecheap identified as receiving the emails sent to *emailreplysecurity.com* addresses was also identified as an account linked to *judejude754@gmail.com* because it has the same Recovery email address listed (*water4all25@yahoo.com*) and the same SMS number (+2349094642540).

26. In summary, the IP address found in the fraudulent emails sent to J.D and T.D. (45.35.132.200) is connected to the Web Pundits user "Lord Iphie" with email address *uzohifeanyi@outlook.com*. Several emails from the *uzohifeanyi@outlook.com* account contained IFEANYI's name, passport, address, email address, or phone number. The IP address found in the fraudulent emails sent to K.T. and T.T. matched the IP address (154.73.11.9) used by the Tizeti user "Ikenna Okeke" with phone number +2348038879545 and address 4A, James Anyachae str, Chevron estate. The WhatsApp account associated with phone number +2348038879545 has the same description as the WhatsApp account associated with +2349094642540, the phone number IFEANYI listed on his U.S. visa application. The address "4A, James Anyachae str, Chevron estate", is one unit different from the address IFEANYI listed on his U.S. visa application. The email address fraudulently configured to receive copies of all of J.D.'s emails, *judejude754@gmail.com*, is associated with the phone number listed on IFEANYI's U.S. visa application (+2349094642540). Additionally, the *judejude754@gmail.com* email account is linked to IFEANYI's wife's email account

[11] A "cookie" is a small piece of text that a website can send to a user's Internet browser for a variety of purposes. Cookies allow the websites visited, such as Google.com or Gmail.com, to recognize the electronic device when it returns to the website later, and then tailor the user's online experience accordingly. For example, Google's cookies record all of the Google accounts accessed from the same browser on an electronic device, information about those visits, and the user's preferences and other settings.

(*vivian.agbune80@gmail.com*) and to the email account that received emails sent to the domain *emailreplysecurity.com* (*abutrading1@gmail.com*). All of the fraudulent emails sent to J.D., T.D., K.T., and T.T. included email addresses that added the domain *emailreplysecurity.com*.

CONCLUSION

27. As has been shown above, the government's evidence obtained during the course of this investigation establishes probable cause that IFEANYI obtained information, or aided and abetted in obtaining information, from a protected computer, without authorization for purposes of engaging in fraud. IFEANYI sent, or caused to be sent, or aided and abetted in the sending of, fraudulent emails on or about May 23, 2018 to both T.D and J.D. and K.T. and T.T. resulting in significant financial loss.

28. Based on the forgoing, there is probable cause to believe that Jude Uzochukwu IFEANYI violated 18 U.S.C. § 1343 (fraud by wire, radio, or television), 18 U.S.C. § 1030(a)(4) (accessing protected computer in furtherance of fraud), and 18 U.S.C. § 2 (Aiding and Abetting). Accordingly, I respectfully request that the Court issue a criminal complaint and arrest warrant for IFEANYI.

REQUEST FOR SEALING

29. The investigation of the criminal activity discussed above is ongoing and involves multiple targets, many of which have not yet been identified. Moreover, the FBI is not aware of any potential targets that have knowledge of its investigation. Disclosure of the criminal complaint, the arrest warrants, or this application may result in the dissemination of these materials to the targets, who may destroy evidence, flee from prosecution or otherwise evade the investigation. Disclosure of the contents of this affidavit and related documents might have a significant and negative impact on the continuing investigation and might severely jeopardize its effectiveness.

30. Accordingly, I respectfully request that the Court issue an order that the criminal complaint, the arrest warrants, and this application be filed under seal until further order of this Court.

Respectfully submitted,

Jacob Foiles
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on November 16, 2018.

MICHAEL D. NELSON
UNITED STATES MAGISTRATE JUDGE